

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

| | | |
|--------------------------|---|--------------|
| Cody Clark, on behalf of |) | |
| himself and all others |) | |
| similarly situated, |) | |
| |) | |
| Plaintiff, |) | |
| |) | |
| |) | |
| v. |) | No. 23 C 695 |
| |) | |
| |) | |
| Microsoft Corporation, |) | |
| |) | |
| Defendant. |) | |

Memorandum Opinion and Order

Plaintiff Cody Clark brings this putative class action against Microsoft Corporation ("Microsoft"), alleging violations of sections 15(a)-(d) of the Illinois Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp. Stat. 14/1 *et seq.* Microsoft now moves under Federal Rule of Civil Procedure 12(b)(6) to dismiss each of Clark's claims. I have subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). For the following reasons, the motion is granted in part and denied in part.

I.

According to the complaint, while Clark worked as a salesperson for CONMED, he used "video-based coaching" software

provided by Brainshark, Inc. ("Brainshark"). Compl., ECF 1-1 ¶¶ 8, 45. That software allows a salesperson to record a video of himself and upload it to Brainshark's platform, which then automatically generates feedback about his "elevator pitch." *Id.* ¶ 9. To provide this feedback, Brainshark's software analyzes facial expressions using facial geometry scans from the uploaded video. *Id.* ¶¶ 9-10.¹

Brainshark's software allegedly "interfaces with and/or integrates" two Microsoft products: its Azure cloud services ("Azure") and Azure Cognitive Services applications ("ACS"). *Id.* ¶ 8. "Public cloud[s]" like Azure "allow[] users to, *inter alia*, build and deploy applications; store data; deliver software on demand; and analyze data using machine learning and artificial intelligence." *Id.* ¶ 7. ACS "help[s] developers build cognitive solutions (that can see, hear, speak, and analyze) into their applications." *Id.*

In addition to the allegations in the complaint, Microsoft requests that I take judicial notice of its Products and Services Data Protection Addendum ("DPA"), ECF 16-1, which it says applies to Azure and ACS. Clark does not oppose consideration of this document, and in fact uses it in some of his arguments. Because the document is publicly available, it is a "matter of public

¹ A BIPA case against Brainshark in this district was recently dismissed by stipulation of the parties. See *Wilk v. Brainshark, Inc.*, No. 1:21-cv-4794 (N.D. Ill. July 26, 2023), ECF 57.

record,” and I will take judicial notice of it for purposes of this motion to dismiss. See *U.S. ex rel. Suarez v. AbbVie, Inc.*, 503 F. Supp. 3d 711, 721-22 (N.D. Ill. 2020) (citing *Cause of Action v. Chi. Transit Auth.*, 815 F.3d 267, 277 n.13 (7th Cir. 2016)).

II.

“To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “A claim is facially plausible ‘when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.’” *Law Offs. of David Freydin, P.C. v. Chamara*, 24 F.4th 1122, 1128 (7th Cir. 2022) (quoting *Iqbal*, 556 U.S. at 678). I accept well-pleaded facts as true and draw all reasonable inferences in plaintiff’s favor, but I am “not bound to accept legal conclusions as true.” *Burger v. County of Macon*, 942 F.3d 372, 374 (7th Cir. 2019) (citations omitted).

A.

Section 15(b) regulates entities that “collect, capture, purchase, receive through trade, or otherwise obtain” biometric

data.² 740 Ill. Comp. Stat. 14/15(b). Microsoft maintains that Clark's section 15(b) claim should be dismissed because he failed to plausibly allege that Microsoft took an "active step" to obtain his biometric data. In response, Clark focuses only on whether Microsoft "receive[d] through trade" or "otherwise obtain[ed]" the data, and argues that section 15(b) does not require an active step and that, in any event, he has plausibly alleged one.

I agree with Microsoft and the weight of authority in this district that section 15(b) liability requires an active step in obtaining biometrics. *See, e.g., Jones v. Microsoft Corp.*, No. 22-cv-3437, 2023 WL 130495, at *3 (N.D. Ill. Jan. 9, 2023) (applying "active step" requirement to section 15(b) claim); *Patterson v. Respondus, Inc.*, 593 F. Supp. 3d 783, 824 (N.D. Ill. 2022) (same); *King v. PeopleNet Corp.*, No. 21 CV 2774, 2021 WL 5006692, at *8 (N.D. Ill. Oct. 28, 2021) (same); *Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C 866, 2021 WL 3172967, at *2 (N.D. Ill. July 21, 2021) (same). The Illinois legislature premised BIPA sections 15(a), (c), (d), and (e) on "possession" of biometrics, but chose not to use that term in section 15(b). That choice matters. *See Chi. Teachers Union, Local No. 1 v. Bd. of Educ. of the City of*

² Though BIPA defines "biometric identifier" and "biometric information" independently, see 740 Ill. Comp. Stat. 14/10, I use them interchangeably in this opinion, along with the terms "biometric data" or "biometrics." The terms' distinctions make no difference for present purposes.

Chi., 963 N.E.2d 918, 925 (Ill. 2012) (“When the legislature includes particular language in one section of a statute but omits it in another section of the same statute, courts presume that the legislature acted intentionally and purposely in the inclusion or exclusion, and that the legislature intended different meanings and results.” (citations omitted)).

The term “otherwise obtain” is also best construed as requiring something beyond passive possession or receipt. The parties put forth dueling dictionary definitions of the word “obtain”—Microsoft’s preferred definition makes the verb active, while Clark’s makes it passive. *See Obtain, Black’s Law Dictionary* (11th ed. 2019) (“[t]o bring into one’s own possession; to procure, esp. through effort”); *Vance v. Microsoft Corp.*, 525 F. Supp. 3d 1287, 1297 (W.D. Wash. 2021) (“‘[t]o come into the possession of,’ or ‘to get, acquire, or secure’” (quoting *Obtain, Oxford English Dictionary*, https://www.oed.com/dictionary/obtain_v (last visited August 21, 2023))). But because “otherwise obtain” comes at the end of a list of active verbs,³ the more active definition is the better one here. *See Pooh-Bah Enters., Inc. v. County of Cook*, 905 N.E.2d 781, 799 (Ill. 2009) (“[W]hen a statutory clause specifically describes several classes of persons or things and

³ “Receive” alone need not be active, but to “receive through trade” requires the active step of engaging in trade with some other entity.

then includes 'other persons or things,' the word 'other' is interpreted to mean 'other such like.'" (citation omitted)).⁴

Clark cautions that applying an active step requirement to section 15(b) is tantamount to "rewrit[ing] [BIPA] to create new elements or limitations not included by the legislature," in contravention of Illinois Supreme Court caselaw. *Cothron v. White Castle Sys., Inc.*, -- N.E.3d --, 2023 WL 4567389, at *7 (Ill. Feb. 17, 2023). Indeed, according to Clark, the federal courts that had previously observed such a requirement can no longer be considered good law after *Cothron*. But *Cothron* merely reiterated rules of statutory construction that have been around for many years, and certainly since BIPA has been enacted. While true that section 15(b) nowhere says the words "active step," the statutory construction offered above shows that, "[u]nder a commonsense reading," "the private entity must undertake some effort to collect or obtain biometric identifiers or information." *Jones*, 2023 WL 130495, at *3; see *id.* ("[T]his concept simply describes the unifying characteristic among the verbs in the statute.").

The complaint does not sufficiently allege that Microsoft took an active step in obtaining Clark's biometric data. There are

⁴ As for Clark's argument that Microsoft receives his biometrics through trade, the complaint lacks allegations of a "transaction or swap" by which Microsoft received biometrics. See *Trade, Black's Law Dictionary* (11th ed. 2019). Instead, I agree with Microsoft that the allegations suggest it provided its technology in exchange for payment by Brainshark. See Compl. ¶¶ 33-34.

repeated allegations that, for Brainshark to conduct its analysis of sales employees, it “(1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of such individuals’ biometric identifiers (namely, scans of facial geometry) and biometric information.” Compl. ¶¶ 10, 40; *see also id.* ¶ 46 (similar). From there, Clark alleges that because “Brainshark’s software interfaces with and/or integrates Azure and/or ACS, Defendant Microsoft also (1) collects, captures, and/or otherwise obtains; (2) stores; and/or (3) makes use of such individuals’ biometric identifiers and biometric information.” *Id.* ¶¶ 11, 41; *see also id.* ¶¶ 13, 43, 47 (similar). That alone is a conclusory jump, and the complaint does not elsewhere allege facts sufficient to draw the inference that Microsoft actively obtained Clark’s biometrics. Indeed, the complaint makes clear that Microsoft provides technology to Brainshark and that Brainshark allegedly uses that technology to collect Clark’s biometrics. *See, e.g., id.* ¶ 7 (alleging that Azure is “a public cloud” that “allow[s] users to” perform various tasks (emphasis added)); *id.* ¶ 29 (describing ACS as “cloud-based artificial intelligence (AI) services that help *developers* build cognitive intelligence into applications” and “easily add cognitive features into *their* applications with cognitive solutions that can see, hear, speak, and analyze” (emphasis added) (footnote and internal quotation marks omitted)); *see also id.* ¶¶ 28, 30–32.

Rivera v. Amazon Web Services offers a helpful contrast. No. 2:22-cv-00269, 2023 WL 4761481 (W.D. Wash. July 26, 2023). There, the court found sufficient for section 15(b) purposes the plaintiff's allegations that the defendant could "access" and "extract" biometric data uploaded by an intermediary, and that it was "involve[d] in the data collection process . . . beyond simply providing the technology to" another entity. *Id.* at *5; see also *Mayhall ex rel. D.M. v. Amazon Web Servs., Inc.*, No. 2:21-cv-01473-TL, 2023 WL 2728292, at *1, *3 (W.D. Wash. Mar. 31, 2023) (finding active step where defendant "use[d] its computing power . . . to collect facial features vectors from face-scan data," "construct[ed] a 3D face geometry of the user," and "transmit[ted] the [f]ace [g]eometry to [video game] players' [g]aming [p]latforms"). Clark's other cases are similarly distinguishable because in those cases, the defendants allegedly played active roles in obtaining biometrics. For example, in *Johnson v. NCR Corp.*, the court upheld a section 15(b) claim where the plaintiff alleged the defendant actively managed, maintained, and stored biometric data and that defendant's system itself captured the biometrics in the first place and used them to create templates that could be employed for identification purposes. No. 22 C 3061, 2023 WL 1779774, at *4 (N.D. Ill. Feb. 6, 2023). Here, as far as I can tell from the complaint, Microsoft provided technology to Brainshark, plus storage. That is not an active step. See *Jones*,

2023 WL 130495, at *4 (finding providing storage did not constitute “active step”); *Jacobs*, 2021 WL 3172967, at *3 (finding provision of technology did not constitute “active step”); *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019) (same).⁵

Nor does the DPA help. Many of the portions Clark cites describe what Microsoft does with data in its possession, but as explained above, possessing data does not suffice for a section 15(b) claim. And though the DPA at one point references how “Personal Data processed by Microsoft in connection with providing the Products and Services is obtained,” DPA at 8, the DPA goes on to indicate that some such data is “sent to” Microsoft, *id.*, which would not constitute an active step. In any event, the complaint is silent on whether Microsoft “processes” the alleged biometric data at issue here. Additionally, as used in the DPA, “obtained” could assume its passive, rather than active, meaning. I would need to make more than one speculative leap to infer that Microsoft took an active step to obtain Clark’s data based on the DPA.

⁵ In his response brief, Clark argues that Brainshark “has to provide the relevant videos to Microsoft, from which Microsoft extracts biometric data using” Azure and ACS “before returning the biometric data to Brainshark.” Resp., ECF 24 at 10 (citing Compl. ¶¶ 13, 28, 33, 37–43). I do not understand the cited paragraphs of the complaint to support that contention. To the extent he has a good faith basis to allege that is what actually happens--that is, that Brainshark sends the videos to Microsoft, Microsoft extracts biometric data, and then sends the biometric data back to Brainshark--he should so allege in any amended complaint.

B.

Clark's remaining claims, under sections 15(a), (c), and (d), each require that Microsoft was "in possession of" Clark's biometrics. 740 Ill. Comp. Stat. 14/15(a), (c), (d). The parties agree that the ordinary meaning of "possession" applies here, which is "the act or condition of having in or taking into one's control or holding at one's disposal.'" *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005) (quoting Webster's Third New International Dictionary 1770 (1986)).

Considering the DPA, it is plausible that Microsoft was "in possession" of Clark's biometric data. The DPA states that Microsoft "control[s] access to Customer Data and Professional Services Data (including any Personal Data therein)." DPA at 9.⁶ In its reply brief, Microsoft does not address this portion of the DPA. And because the complaint alleges that Brainshark is hosted on Azure's servers, see Compl. ¶ 35, I can reasonably infer that the biometric data allegedly collected by Brainshark was on Microsoft's servers and that, once there, Microsoft exercised some degree of control over access to that data. While data storage alone may be insufficient, storage of data together with the

⁶ The DPA defines "Customer Data" to include "video" or "image files" "that are provided to Microsoft by" customers. DPA at 5. "Personal Data" includes information "specific to the physical [or] physiological . . . identity" of a natural person. *Id.*

ability to control access to that data adequately pleads possession.

C.

Microsoft independently attacks Clark's section 15(c) claim, asserting the complaint does not sufficiently allege that Microsoft "sell[s], "lease[s], trade[s], or otherwise profit[s] from" his biometrics. 740 Ill. Comp. Stat. 14/15(c). According to the complaint, Microsoft profited from Clark's data by using it to "further refine its technologies and/or provide services to its clients." Compl. ¶ 73.

But Clark has not sufficiently alleged an injury-in-fact to confer Article III standing with respect to this claim. "Standing is an element of subject-matter jurisdiction in a federal civil action," *Moore v. Wells Fargo Bank, N.A.*, 908 F.3d 1050, 1057 (7th Cir. 2018), and though Microsoft does not argue for dismissal or remand of this claim on those grounds, courts "have an independent obligation to determine whether subject-matter jurisdiction exists, even in the absence of a challenge from any party," *Arbaugh v. Y & H Corp.*, 546 U.S. 500, 514 (2006) (citation omitted). The Seventh Circuit has characterized section 15(c) as a "general regulatory rule" that "no one may profit in the specified ways from another person's" biometric data, and that pleading a bare violation of this provision is not enough for standing purposes. *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1246-47 (7th Cir.

2021). In *Thornley*, the Seventh Circuit held that a section 15(c) plaintiff must allege more than that the defendant profited from their data; they must allege how that conduct harmed them individually. *Id.* at 1247. The Seventh Circuit identified examples of allegations a plaintiff could allege to establish injury-in-fact, like, “for example, that by selling her data, the collector has deprived her of the opportunity to profit from her biometric information”; “that the act of selling her data amplified the invasion of her privacy that occurred when the data was first collected, by disseminating it to some unspecified number of other people”; or that defendant’s use of the biometric data “raise[d] the cost” of using some other product or service, like a social media website. *Id.*

Clark’s complaint fails to plausibly allege more than a bare statutory violation of section 15(c). Indeed, courts in this district have found allegations like those in Clark’s complaint insufficient for standing. *See, e.g., Gorgas v. Amazon.com, Inc.*, No. 22 CV 5159, 2023 4173051, at *2 (N.D. Ill. June 23, 2023) (dismissing claim where allegation was that “Amazon profits . . . by using this biometric data to improve the Rekognition technology that Amazon uses itself and also sells to [various organizations]”); *Hogan v. Amazon.com, Inc.*, No. 21 C 3169, 2022 WL 952763, at *7 (N.D. Ill. Mar. 30, 2022) (same where allegation was that Amazon “used the images uploaded to Amazon Photos to train

Rekognition, which it then sold to third parties"); *Patterson*, 593 F. Supp. 3d at 816 (same where allegation was that defendant profited from biometric data by marketing their product). Even if Microsoft used Clark's data to improve Azure and ACS, which it sells to other entities, that does not explain how doing so harmed Clark.

D.

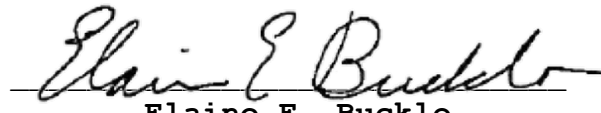
Finally, Microsoft argues that Clark's section 15(d) claim fails because the complaint does not support that Microsoft "disclose[d], redisclose[d], or otherwise disseminate[d]" Clark's data. 740 Ill. Comp. Stat. 14/15(d). I agree. In his brief, Clark characterizes the requisite conduct as "Microsoft's disclosure or dissemination of the biometric data to Brainshark so that Brainshark could provide its services," Resp. at 19, a statement for which he cites to complaint paragraphs 33-35 and 46-49. I take those allegations to mean that Microsoft provides its Azure and ACS technology to Brainshark and other customers, but nothing in those allegations indicates disclosure, redisclosure, or dissemination of biometric data from Microsoft to Brainshark. See *Jones*, 2023 WL 130495, at *5 (dismissing section 15(d) claim where no allegation that defendant disseminated data to "any third-party data centers or any tangible third parties whatsoever"). And the fact that the DPA states that "Microsoft may hire Subprocessors to

provide certain limited or ancillary services on its behalf,” DPA at 11, does not bring this claim from speculative to plausible.

III.

For the foregoing reasons, Microsoft’s motion is denied with respect to Clark’s section 15(a) claim. Clark’s claims under section 15(b) and (d) are dismissed without prejudice for failure to state a claim. *See O’Brien v. Vill. of Lincolnshire*, 955 F.3d 616, 628 (7th Cir. 2020) (noting plaintiff should usually have at least one opportunity to amend). His claim under section 15(c) is dismissed without prejudice for lack of subject-matter jurisdiction. *See Lauderdale-El v. Ind. Parole Bd.*, 35 F.4th 572, 576 (7th Cir. 2022) (“Dismissals for lack of subject-matter jurisdiction are necessarily without prejudice.” (citation omitted)). To the extent Clark is able, consistent with Federal Rule of Civil Procedure 11, to remedy the issues I identify above, he may file an amended complaint within 30 days of entry of this memorandum opinion and order. If no amended complaint is filed by then, his claims under sections 15(b) and (d) will be dismissed with prejudice and the section 15(c) claim will be severed and remanded to state court.

ENTER ORDER:

A handwritten signature in black ink, reading "Elaine E. Bucklo", written over a horizontal line.

Elaine E. Bucklo

United States District Judge

Dated: August 21, 2023